REMARKS

The Examiner is thanked for the thorough examination of the present application. The Office Action, however, has tentatively rejected all claims 1-36. In response, Applicant submits the foregoing amendments and following remarks. In this submission, claims 1 and 31 have been amended to clarify the combination of elements which define broader novel embodiments of the presently pending claims, and claims 8-22 and 24-36 have been amended based on claims 1 and 31.

The Office Action objected to various claims for various noted informalities. Applicant has made appropriate amendments to the claims to address and overcome each of the noted informalities. As amended herein, all claims are blieve to properly overcome the noted objections.

The Office Action also rejected claim 31 under 35 U.S.C. § 101. In response, Applicant has amended claim 31 and as amended, Applicant submits that claim 31 fully complies with all statutory requirements, including the requirements of 35 U.S.C. §101.

Turning now to the prior art based rejections, the Office Action rejected claims 1-36 under 35 U.S.C. § 103 (a), as allegedly unpatentable over U.S. Patent Applications No. 6,490,683 (Yamada) and US 2001/0044887 (Ohgake), in view of rearrangement of functions and further in view of an obvious need. Before discussing the prior arts relied upon by the Examiner, it is believed beneficial to first briefly review the method of the claimed embodiments of the present application, as now defined.

The invention of claim 1 of the present application is directed to a method for encoding and decoding confidential optical disk. The method includes the step of receiving signal of creating confidential optical disk to switch burner into a burning mode. The method also includes the step of setting a data-accessing password for future verification. The method further includes the step of selecting one of data sources for public viewing and confidential viewing data to be burned on the disk. The method includes the step of receiving a start burn signal to begin data encoding process. The method includes the steps of creating a temporary file system as buffer that includes two stages, and creating standard file set and creating parallel file set with real data. Still further, the method includes the step of burning buffer to an optical disk and producing a tangible disk.

In contrast, Yamada is directed to an optical disk having electronic watermark, reproducing apparatus thereof and copy protecting method using the same. Yamada discloses that data has a copy protecting password, *i.e.* the electronic watermark data that is generated based on a user password and is used to avoid dishonest copying (see lines 41-46, Col. 19). Yamada further discloses that both the user password in the file identifier descriptor FID and the password in the electronic watermark data are read out and compared to each other when reproducing data from the data recording medium (see lines 66-67, Col. 19 and lines 1-3, Col. 20).

In addition, Ohgake is directed to a record medium and method of controlling access to record medium. Ohgake discloses that the disclosure level indicates a level specifying an information area in the optical disk 1_{new} accessible by each user, such as

a confidential level to each user, or a usage area corresponding to payment made by each user to contents of the optical disk 1_{new} (see lines 1-5 of paragraph [0030]).

Unlike the claimed embodiments of the present application, as any skilled artisan would appreciate, the electronic watermark data is only used for protecting from dishonest copying or avoiding forging the contents of the file data, but is not used for avoiding unauthorized persons from reproducing confidential data from record medium. Moreover, the disclosure level is used for determining whether a user who wants to access the record medium is an authorized or permitted user, but is not used for specifying that the data is public viewing or confidential viewing data (see lines 8-10 of paragraph [0038]).

Thus, nowhere do the references disclose or suggest setting a data-accessing password that is used for accessing data in the reading process, and selecting one of data sources for public viewing and confidential viewing data to be burned on the disk, as now claimed.

Specifically, claim 1 recites:

> 1. A method for encoding a confidential optical disc with a burner, the method comprising the steps of:
> receiving signal of creating confidential optical disc to switch burner into a burning mode;
> ***setting a data-accessing password for future verification;***
> ***selecting one of data sources for public viewing and confidential viewing data to be burned on the disc;***
> receiving a start burn signal to begin data encoding process;
> creating a temporary file system as buffer that includes two stages, creating standard file set and creating parallel file set with real data;
> burning buffer to an optical disc and produce a tangible disc.

(*Emphasis added.*) Claim 1 patently defines over the cited art for at least the reason that the cited references (alone or in combination) fail to disclose at least the features

emphasized above. As the reference fails to disclose or suggest the combination of elements which form the invention of the subject Patent Application, it cannot make obvious that invention.

As claims 2-30 depend from claim 1, these claims define over the prior art for at least the same reasons. Moreover, ***especially the dummy data or public viewing data of Claims 1, 14, 23, and 30 can be read by anyone and is different from the dummy pack 89 of U.S. Patent Application No. 6,907,187 (Ando), wherein the dummy pack 89 is used for allowing users to edit the contents of the recording after having recorded the video title set VTS in lines 16-23, Col. 11 of Ando.***

Furthermore, the Official Action rejected claims 31 and 33 under 35 U.S.C. § 103(a), as allegedly unpatentable over U.S. Patent Applications No. 6,490,683 (Yamada), US 2001/0044887 (Ohgake) and No. 6,954,862 (Serpa), in view of rearrangement of functions and further in view of an obvious need. Before discussing the prior art relied upon by the Office Action, it is believed beneficial to second briefly review the method of the embodiment defined in claim 31.

The embodiment of claim 31 is directed to a method for reading a confidential optical disk. The method includes the step of reading optical disk data. The method also includes the step of receiving view confidential data command signal. The method further includes the step of requesting to enter password. The method includes the step of checking if password entries reach a predetermined limitation. The method includes the steps of checking if correct ID field exists if password entries do not reach the predetermined limitation. The method further includes the step of checking if entered password is correct if ID field exists in the optical disk. The method also includes the

step of playing/reading real data if entered password is correct. Still further, the method includes the step of ending playing/reading session.

In contrast, Yamada discloses that when reading data from recording medium, both the user password in the file identifier descriptor FID and the password in the electronic watermark data are read out and compared to each other (see lines 66-67, Col. 19 and lines 1-2, Col. 20).

Ohgake discloses that the disclosure level indicates a level specifying an information area in the optical disk 1_{new} accessible by each user (see lines 1-5 of paragraph [0030]). Ohgake discloses that the record-medium accessing software 12 determines the optical disk 1 is the peculiar optical disk 1_{new} if the optical disk 1 includes the record-medium identification information "d", and requests a user to input a password, as well as the disclosure level "n", for determining whether the user is an authorized or permitted user (see lines 1-10 of paragraph [0038]). Ohgake discloses that the record-medium accessing software 12 decides whether the optical disk 1 includes the record-medium identification information "d" (see lines 4-11 of paragraph [0037]).

In addition, Serpa discloses that the number of incorrect login attempts is often limited, such as to three attempts.

Unlike the embodiment of claim 31, as will be appreciated by persons skilled in the art, the electronic watermark data is only used for protecting from dishonest copying but is not used for avoiding that unauthorized person reproduces confidential data from record medium, wherein the electronic watermark is generated by the user password (see lines 29-46, Col. 19). Moreover, in Ohgake, the software first performs the step of

deciding whether the optical disk 1 includes the record-medium identification information "d", and then performs the steps of requesting user to input qualification information and checking whether the qualification information is correct.

In fact, the references teach away from the method of the claimed embodiments, in that the qualification information of Ohgake is used for determining whether the user who enters the qualification information is authorized, and deciding the information area of the optical disk for the user. The electronic watermark data of Yamada is only used for protecting from dishonest copying or avoiding forging the contents of the file data, but is not used for avoiding that an unauthorized person reads confidential data from record medium.

Whereas, in the claimed embodiments, the password is used for allowing authorized users to read real data stored in the optical disk. The player first checks if any correct ID field exists and then checks if the entered password is correct for further reading real data. On the other hand (see lines 29-33 of page 9 of the present specification), users can access both of real data and dummy data if the entered password is correct, and users can only access dummy data if the entered password is incorrect.

Thus, nowhere do the references disclose or suggest playing/reading real data if entered password is correct, as now claimed. As the reference fails to disclose or suggest the combination of elements, which define the claimed embodiments, it cannot render the claimed embodiments obvious.

Specifically, claim 31 recites:

31. A method for reading a confidential optical disc, which is a decoding method for reading optical disc produced by claim 1, the method comprising steps of:
player reading optical disc data;
receiving view confidential data command signal;
requesting entry of a password;
checking to determine if password entries reach a predetermined limitation;
if password entries do not reach the predetermined limitation, checking if correct ID field exist;
if ID field exists in the optical disk, checking if entered password is correct;
if entered password is correct, playing/reading real data;
ending playing/reading session.

(*Emphasis added.*) Claim 31 patently defines over the cited art for at least the reason that the cited art fails to disclose at least the features emphasized above.

For at least the foregoing reasons, it is believed that the present application has been placed in condition for allowance and such action is respectfully requested.

CONCLUSION

In view of the foregoing, it is believed that all pending claims are in proper condition for allowance.

Should the Examiner have any questions regarding this response, the Examiner is invited to telephone the undersigned attorney at (770) 933-9500.

No fee is believed to be due in connection with this amendment and response to Office Action. If, however, any fee is believed to be due, you are hereby authorized to charge any such fee to deposit account No. 20-0778.

Respectfully submitted,

/Daniel R. McClure/

Daniel R. McClure
Registration No. 38,962

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500